09/269618

PCT/GB 97/02512

The Patent Office

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP9 1RH

REC'D 21 OCT 1997
WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

PRIORITY DOCUMENT

Signed G D Court

Dated -3 OCT 1997

This Page Blank (uspto)

Patents Form 1/77

Patents Act 1977
(Rule 16)

THE PATENT OFFICE
26 SEP 1996
RECEIVED BY HAND

The Patent Office

DY & CO

30SEP96 E223406-24 D00244
P01/7700 25.00

Request for a grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1.	**Your reference**	P\1020.GB MKH — 26 SEP 1996
2.	**Patent application number** *(The Patent Office will fill in this part)*	**9620079.5**
3.	**Full name, address and postcode of the or of each applicant** *(underline all surnames)*	Mr. Richard Billingsley 17/38 Glebe Street Randwick 2031 New South Wales Australia
	Patents ADP number *(if you know it)*	7072135001
	If the applicant is a corporate body, give the country/state of its incorporation	
4.	**Title of the invention**	IMPROVEMENTS RELATING TO ELECTRONIC TRANSACTIONS
5.	**Name of your agent** *(if you have one)*	D YOUNG & CO
	"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*	21 NEW FETTER LANE LONDON EC4A 1DA
	Patents ADP number *(if you have one)*	59006

6. **If you are declaring priority from one or more earlier patent applications, give the country and date of filing of the or each of these earlier applications and (if you know it) the or each application number**

Country	Priority application number *(if you know it)*	Date of filing *(day/month/year)*

7. **If this application is divided or otherwise derived from an earlier UK application, give the number and filing date of the earlier application**

Number of earlier application	Date of filing *(day/month/year)*

8. **Is a statement of inventorship and of right to grant of a patent required in support of this request?** *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

NO

9. **Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document**

Continuation sheets of this form	0
Description	29
Claims*(s)*	7
Abstract	1
Drawing*(s)*	8

10. **If you are also filing any of the following, state how many against each item.**

Priority documents	0
Translations of priority documents	0
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	0
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	0
Any other documents *(please specify)*	0

11. **I/We request the grant of a patent on the basis of this application.**

Signature D Young & Co.

Date 26.09.96

D YOUNG & CO
Agents for the Applicants

12. **Name and daytime telephone number of the person to contact in the United Kingdom**

Miles K. Holmes 0171 353 4343

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505

b) Write your answers in capital letters using black ink or you may type them

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separte sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

DUPLICATE

IMPROVEMENTS RELATING TO ELECTRONIC TRANSACTIONS

This invention relates to electronic transactions or transfers using an electronic representation of a commodity, such as money. The invention is especially suitable for use in financial transactions, but it is not limited exclusively to such use. The invention is also especially suitable for use over a public communication network, such as the internet, but again the invention is not limited to such use.

With electronic money systems, there are a number of problem areas, as follows:

SECURITY – To prevent fraudulent interference with transactions involving the money. This is particularly important for transactions over public communication systems, such as over the internet, or by electronic mail, where the electronic message necessarily passes through a number of different computer systems, and is vulnerable to copying by thieves. Security is also needed to prevent the same electronic money from being spent twice.

AUTHENTICATION – So that users of electronic money can verify, without needing to contact the bank or other money issuer, that the electronic money they receive is valid (i.e not forged), has not been "spent" already, and will be honoured by the bank or other electronic money issuer.

ANONYMITY – To assure users of the electronic money that the transactions and transfers in which they are involved will, if desired, remain confidential, in the same manner as cash transactions, and will not be tracked by banks or other bodies who might be interested in users' spending habits. Further, neither current users nor new users should have to provide any personal information which might reveal their true identity to the bank or to any other electronic money handling or regulating authority.

AUDITABILITY – To reassure the bank or the money issuer that electronic money which they receive for redemption did, in fact, originate from that bank and has not been issued by some other issuer or possibly forged with the aid of confidential bank information.

DIVISIBILITY – To enable a user of the electronic money to spend a portion of the money, or to obtain change as part of the transaction. It would also be desirable to accommodate fractions of a denomination of money, and to facilitate money transfers from one currency to another without concerns over denomination.

NON-AFFILIATION – To permit a user to possess, receive and spend the electronic money without the need to be registered with, or have an account with, a particular bank or other electronic money issuer. Further, the user should preferably not have to provide any third party with any personal information from which the person's identity could be ascertained, or which would need to be updated if the person were to move residence, or to get married, for example.

TRANSFERABLE – To enable the electronic money to be transferred to anyone independently of the type of transaction or transfer, and regardless of whether the parties are commercial bodies or private individuals.

INDEPENDENCE – To enable electronic money to be spent and received independently of the location of the parties to the transaction. For example, the parties may be in the same physical location, or they may be in completely different locations.

OFFLINE PAYMENT – To enable the electronic money to be transferred without needing simultaneously with the bank at the time of transfer.

NON-LIABILITY – Particularly when communicating over a public communication system, there are occasions when communication is interrupted, or a message is not confirmed as having been received, or a computer system crashes. In such a situation, it may be impossible to establish whether an instructed electronic money transaction or transfer has taken place. In other situations, data representing the electronic money might be lost. It is desirable that an electronic money user to be able to repeat the same transaction, or make "back-up" copies of the electronic money, without increasing the liability of the user and the bank.

One example of a known electronic money system is "e-cash". In that system, electronic coins of fixed denomination are represented by serial numbers. When the serial numbers are transmitted to a third party, they can be redeemed at an issuing bank. However, with such a system, it is difficult for a person receiving money to verify, without contacting the issuing bank, that the money has not previously been doubly spent (either accidentally, or deliberately). The money is only authenticated by the bank when the receiver of the money attempts to redeem it at the bank. Furthermore the system does not provide divisibility of the electronic money, since the denominations of the coins are fixed. The electronic coins are also difficult to track by the bank to identify forged electronic coins, ie. coins which may look valid but which were not issued by the same issuing bank.

US-A-5511121 describes a system which allows a bank to detect the double spending of an electronic coin when the coin is redeemed twice, by using a El Gamal signature function. However, such a system relies on the identity of the user being derivable from the user's key, which necessitates the user being registered with a central authority. Furthermore, the system does not enable a receiver of the electronic coins the ability to verify that the coins are valid before the receiver accepts the coins as payment; it merely enables the detection of double spending when the same coin is redeemed at the bank by two or more users. Furthermore, if a communication involving the electronic money needs to be repeated or modified, there is risk that the double signatures which result will yield the identity of the spender, and possibly create an embarrassing situation in which the spender may be accused of fraudulently spending the coin twice.

Reference is also made to EP-A-0139313 which describes a method of transforming or "blinding" a message to be signed into a form which obscures the content of the message for signature, but which retains the signature relationship when transformed back to the original message, even though the result is not readily associated with the transformed message.

The present invention has been devised bearing the above problem areas in mind.

The present invention proposes the use of "value notes", which can be in the form of

electronic messages, and represent a commodity, such as money. A value note is similar to a note of conventional currency in that it is promise by the note issuer to provide the bearer with the commodity on redemption of the value note. For example, if the value note represents money, then it is equivalent to cash in the bearer's hand.

The invention uses digital signatures, which are calculated by a signatory when "signing" or endorsing the value note. Each signature may be regarded as an encoded checksum or hashing function which is dependent on information in the value note (e.g. certain message text), and is dependent on a secret key known only to the signatory. The signature function is such that, without knowing the signatory's secret key, it is very difficult (and preferably impossible for practical purposes) to forge or decode the signature. However, with a given message and a given signature, it is possible to verify whether the signature matches the message. This is enabled by a public key for the signatory which may, for example, be included with the digital signature. The public key is such that, although it does not provide sufficient information to correctly calculate a signature for a message (the secret key is required for this), it does provide sufficient information to enable an independent verification to be made as to whether the signature matches the message.

The public key is derived from the secret key by a special function which is very difficult or impossible to reverse (making it safe to publicly disclose the public key to other parties without risk that the secret key will be discovered).

In accordance with one aspect of the invention, a value note comprises, or presents, information consisting of:

first information representative of public key information for a bearer;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and public key information for the issuer.

With this aspect of the invention, a value note is secure and is easily verifiable by the bearer independently of the issuer. The value note is secure because the issuer's signature

protects the public key information and the commodity information to prevent it from being altered. Should either or both of these items of information be altered, then the issuer's signature will no longer match the altered information, and this is easily verifiable by the bearer without having to contact the issuer.

The issuer's public key information is required to enable the verification to be carried out. This information could be included as part of the information in the value note. Additionally or alternatively, the issuer's public key information may be published, for example, in journals or newspapers, or it may be published over an electronic communication system, for example, over the internet.

Before a value note can be obtained, a bearer first has to select or generate a secret key and a public key as described above. The bearer keeps the secret key confidential and supplies the public key information to the value note issuer for inclusion as the first information in the value note. This information will be used later to verify whether the bearer's signature is correct when the value is redeemed (in a similar manner to that used on travellers cheques). By using a public key in this way, the bearer can remain anonymous since the public key information does not have to identify the bearer. The signature key information can be chosen arbitrarily by the bearer; it does not need to be assigned to him, or be "registered" with, a bank or other governing authority. The bearer is also free to alter his signature information from one value note to another, and to use different signature information on different concurrent value notes.

In order to redeem the value note, a bearer can append redemption instruction information to the note and then endorse the note and/or the payment instruction information with a digital signature (using the secret key from which the public key information has been derived). The bearer may then communicate the endorsed value note back to the issuer for redemption.

It will be appreciated that only the original bearer will be able to "write" or calculate a correct signature with the knowledge of the secret key. The use of a bearer's signature in this way provides two advantages. Firstly, it guarantees that the value note has been endorsed

by the true bearer, without revealing the identity of the bearer. Secondly, it guarantees that the bearer's redemption instructions have not been altered fraudulently. These advantages arise because the bearer's signature will only be verifiable using the public key information already included in the value note if:

(i) the signature has been generated using the same secret key used to generate the public key; and

(ii) the redemption instructions are identical to those at the time the signature was calculated.

Therefore, it is safe to transmit value notes and payment instructions openly over a public communication system. Should a thief attempt to alter the redemption instructions, or to forge the signature, this will be immediately apparent to the issuer who can then take appropriate action. Furthermore, should a value note go astray in an electronic communication system, then either the issuer of the bearer can simply send a duplicate value note without increasing either the issuer's liability or the bearer's liability.

It will be appreciated that the security for each digital signature is dependent on the length of the signature information. With the invention, the liability at the time of signing lies with the signing party, and the onus is on the signing party to provide an appropriately secure signature to avoid increased liability. In other words, when an issuer (e.g. issuing bank) signs a blank value note to create an issued value note, the onus is on the bank to provide a signature which is sufficiently long to be undecodable for practical purposes. If the bank's signature is insufficiently long such that other parties can forge value notes, then the increased liability lies with the bank who will have to honour any value notes bearing a matching signature. Similarly, when a bearer signs a value note (for redemption), the onus is on the bearer to provide a sufficiently long signature information (for example the public key), to make the signature secure. If the signature is insufficiently long, other parties may be able to forge the bearer's signature. The increased liability therefore lies with the bearer, not the issuing bank, because the bank has only to honour the first presentation of a value note with a matching bearer signature.

The endorsing signature of the bearer should preferably be based on information

including the public keys of the seller (new bearer) and of the buyer (current bearer), so that the public key information cannot subsequently be altered. If the public key information is included in the payment instruction information, then it will automatically be included in the endorsing signature. However, if the public key information is not included in the payment instruction information, then these items of information should be added separately to the information on which the endorsing signature is based.

If desired, a value note may be encrypted before it is sent over a public communication system, as a further precaution for security and anonymity. For example, before communicating a value note to a bank, a bearer might encrypt the value note information using the bank's public key as an encryption key. When received at the bank, the bank computer will be able to decrypt the value note using the bank's secret key as a decryption key.

Preferably, the redemption instructions include a reference to redeem at least a proportion of the commodity in the form of a (first) new value note. Additionally, the redemption instructions may include a reference to redeem the remainder of the commodity (if any) in the form of a second new value note. This provides a convenient technique for transferring the commodity, or a part of the commodity, from one bearer to another. To achieve such a transfer, it is simply necessary for the new bearer (ie. the receiver) to provide his own public key information for inclusion in the new value note intended for him. If desired, the new bearer can communicate this information directly to the value note issuer. However, it is particularly preferred for the new bearer to provide the original bearer with the new public key information, and for the original bearer to communicate with the value note issuer. The new value note will then be issued to the original bearer who can forward the new value note to the new bearer, for example, as a payment. This is advantageous because it avoids the need for any direct communication between the issuer and the new bearer, and hence ensures complete anonymity. The only party who needs to communicate with the new bearer is the original bearer. In may cases, the original bearer may already be aware of the new bearer's identity; however, this is not essential and, in other cases the original bearer may be unaware of the actual identity of the new bearer. In this respect, the transaction can be equivalent to a cash transaction.

Such a technique achieves complete security for the new bearer even though the new value note will be handled by the original bearer. The new bearer will be able verify the authenticity of the new value note independently by means of the value note issuer's signature. Furthermore, it will be impossible for the original bearer to attempt to forge the new bearer's signature because the original bearer will only be aware of the new bearer's public key; the original bearer will not be aware of the new bearer's secret key which is required for writing an endorsement signature.

The above value notes may include additional information such as one or more identification codes or strings for uniquely identifying the value note, and information regarding the date and/or time of creation (issuance) the date and/or time of expiry (ie. the date or time by which the value note must be redeemed if it is to be valid). Preferably, at least some of this additional information (particularly the expiry information) is included as part of the signature calculation, to protect the information from being altered.

The provision of expiry information would be welcomed by financial institutions. It is believed that such institutions may be reluctant to issue value notes of indefinite validity because it would otherwise be difficult to assess an issuer's liability to pay old, unredeemed value notes. Furthermore, the provision of unique identifying information would be welcomed by financial institutions to enable an audit track of a value note to be maintained. This can be used by a bank to verify that the bank is only accepting its own value notes for redemption.

One preferred feature of the invention is that value notes are only issued by one or more value note issuing authorities. For example, where the commodity is money, banks may be the value note issuing authorities. New value notes are not issued directly by the bearers. Therefore, the value note issuing authorities can maintain tight security control over the value notes, and can detect whether fraudulent payment instructions are being received.

Another preferred feature of the invention is the ability of a bearer to issue a redemption instruction for the creation of a first new value note for at least a proportion of the commodity, optionally a second new value note for the remainder (if any) of the

commodity, and optionally a third new value note as a replacement for the first new value note if the first new value note is not redeemed within a predetermined period. In effect, such this is a request for a temporary first new value note with a limited life, after which the first new value note is to be considered useless and is to be replaced by the third new value note.

This can provide an extremely useful technique for temporarily making a commodity available to a new bearer. The predetermined period may be as long or as short as desired. For example, the period may be as short as 30 minutes, or less, or as long as a month or more. This technique can also be used to ensure that if, for any reason, a bearer forgets to redeem his value note before its normal expiry date, the commodity will still be retained by the issuance of a new value note with a new expiry date.

A particularly preferred feature is the ability of a bearer to impose payment conditions or requirements in the third, temporary value note which must be met before the third value note can be redeemed. Therefore, a new bearer will not only have to redeem the temporary third value note before it is due to expire, he will also have to meet the further requirements imposed by the original bearer.

Again this provides an extremely useful technique for a transaction between, for example, a buyer and a seller. The buyer can instruct the creation of a temporary value note in favour of the seller to demonstrate to the seller that sufficient money is available, but subject to certain conditions which the buyer may wish to impose. Generally, the conditions will be verifiable by the bank from the information on the endorsed value note, so that the verification can be performed independently of the buyer and seller. Preferably, the requirement and the verification are signature based.

For example, one condition might be that the buyer himself has to "counter-sign" the temporary value note before it can be redeemed by the seller. This is distinct from a "normal" value note in favour of the seller as described above, which only requires the signature of the seller for redemption. With the additional requirement for a counter-signature, the buyer can delay his signature until, for example, he has received goods or

money from the seller. By counter signing, the buyer confirms that the transaction has been completed, and he makes the temporary value note redeemable.

As an alternative example, the buyer may include a receipt or guarantee message in the temporary value note which the seller will have to endorse with his signature as part of the redemption process. This provides a technique for obtaining a receipt from the seller which has been endorsed by the seller. Preferably, the message is encrypted by the buyer and/or seller so that the bank or other value note issuing authority is unable to read its contents. Such encryption can provide the buyer with a guaranteed receipt for the transaction, but still preserve the anonymity of the transaction. The bank is able to verify that the encrypted text matches the signature information, even though the bank is unable to read the receipt information directly.

As an example, once the buyer has prepared the text message (for example, the receipt message) for the option note, the buyer may "blind" the message by applying a blinding function before the message is signed. A blinding function is a function which renders the message unreadable to a person without knowledge of the blinding key but, when the message is unblinded, it retains its original relationship with the signature. In other words, the blinding function encrypts the message without affecting the verification of the endorsing signature. One example is to multiply the encrypted message by a chosen blinding factor.

If a blinded message is used, and it is desired that the seller be able to read the blinded message, then it is necessary to include the blinding factor as part of the information on the option note. This is done by encrypting the blinding factor in such a way that only the seller can decrypt it. For example, the seller's public signature can be used to encrypt the blinding factor; only the seller with the knowledge of his own secret key will then be able to decrypt the blinding factor. If the blinding factor is encrypted as numeric information, then it should be double encrypted, since it may be possible to ascertain the blinding factor from a single encryption. However, if the blinding factor is encrypted as a text string, then it should only be necessary to encrypt this once, since it will then not be possible to decrypt the text string.

It will be appreciated that the invention achieves distinct technical advantages in enabling secure and anonymous transactions to be conducted openly over a public communication system, such as the internet. In one aspect the invention may be regarded as a protocol defining the manner in which value note information is presented. The above advantages are a direct result of the manner in which information is arranged to form a value note, rather than the content of the information itself.

In various aspects the invention provides methods and apparatus for handling value notes, and representations of value notes.

In one related aspect, the invention provides a method of providing a value note comprising:

providing first information representative of public key information for a bearer;

providing second information representative of a commodity represented by the value note; and

calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of public key information for the issuer.

In another related aspect, the invention provides a method of handling a value note, comprising:

receiving a value note comprising first information representative of a bearer's public key, second information representative of a commodity represented by the value note, and third information representing an issuer's signature which can be verified by information including the first and second information and public key information for the issuer;

providing redemption instruction information for the value note; and

providing a bearer's signature which is dependent on the payment instruction information and is verifiable from said first information.

In a yet further related aspect, the invention provides a method of handling a value note with associated redemption instruction information and bearer signature information, the method comprising performing at least one verification prior to redeeming the value note in accordance with the redemption instruction information, the verification comprising:

verifying that the bearer signature information matches information including at least the payment redemption instruction information using public key information for the bearer presented in the value note.

A further aspect of the invention relates to preventing malicious use of value notes, or other electronic representations of a commodity, by repeatedly attempting to redeem the commodity immediately after issuance. For example, in the case of a value note, a malicious user might try to repeatedly redeem a new value note immediately after issuance in order to try to disrupt the bank's computer. To prevent this, the invention proposes a method wherein an electronic representation of a commodity is issued by an issuing authority, the electronic representation including information representing a time and/or date from which the electronic representation is available for redemption, said time and/or date being later than the time and/or date of issuance, whereby the electronic representation is not available for redemption immediately after issuance. This method is especially suitable when used with a value note as defined hereinbefore, but is also equally suitable for use with other forms of electronic money (or electronic representations of another commodity).

A yet further aspect of the invention relates generally to encrypting information in such a manner that it is decryptable by another authorised party, and is also "verifiable" by a third party even though the third party is not able directly to read the encrypted information. In accordance with this aspect of the invention, this can be achieved by applying a "blinding" function to the information, in a similar manner to that described above, and including an encrypted version of the blinding key of factor.

If the message is received by an "authorised" recipient (i.e. a party who can decrypt the encrypted blinding key in the message), then the recipient can decrypt the blinding key and use that information to "unblind" the blinded information. Even when the information is unblinded, the relationship with the signature is preserved, such that the unblinded message can be verified against the signature. On the other hand, if the message is received by a non-authorised recipient (ie. a party unable to decrypt the blinding key), that party will be unable to read the blinded message directly, but will still be able to verify from the blinded information that it matches the signature.

Embodiments of the invention are now described by way of example only with reference to the accompanying drawings, in which:–

Fig. 1 is a schematic diagram of a system for handling value notes;
Fig. 2 shows an example of a value note issued to a bearer;
Fig. 3 is a flow diagram of the issuing process;
Figs. 4, 5 and 6 show value notes prepared for a transaction;
Fig. 7 is a flow diagram of a process for endorsing a value note for a transaction;
Fig. 8 is a flow diagram of a process for redeeming a value note;
Figs. 9, 10 and 11 show new value notes issued as a result of the redemption process;
Fig. 12 shows an example endorsement of a value note for creating a temporary option note;
Fig. 13 shows an example blank option note;
Figs 14, 15 and 16 show value notes issued as a result of the redemption process;
Fig. 17 shows an endorsed option note; and
Fig. 18 is a partial flow diagram for redeeming an option note.

Fig. 1 shows an illustrative example of the main parts of a system for handling value notes. A bank computer 10 is provided for issuing and honouring value notes. Users of electronic money have computer terminals 12, for example, domestic computer systems, which can communicate with the bank computer 10 by means of a public access network, shown schematically at 14. The network 14 may typically allow access to the bank computer 10 through the internet, or through electronic mail, or other public networks. For brevity, only two user terminals 12 are depicted in Fig. 1; it will be appreciated that the number of terminals which can communicate with the bank computer 10 in this way will be vast. Any computer having access (for example, modem access) to the public communication system 14 may be able to communicate with the bank computer 10.

Digital signatures are used both by the bank and by the users to endorse each value note. In this context, a digital signature is a verifiable code or sequence of numbers which establishes the validity of a piece of text, and acts as evidence that the text has been endorsed by the signatory.

The digital signature S may be expressed as

$$S = f1(m,k)$$

where:

m represents message text to be endorsed by the signature; and

k represents the signatory's secret key.

The signatory also has a public or authorship key A which may be expressed as

$$A = f2(k)$$

The functions f1 and f2 are related such that given a message m, a signature S, and the signatory's public key A, it is possible to verify whether the signature matches the message. On the other hand, the functions f1 and f2 are such that it is impossible to decode a signature or the public key to try to ascertain the secret key. The signature S, the secret key k and the public key A may each consist of one or more numbers, as desired.

As one example, an RSA signature may consist of a number S, and the public key may consist of two numbers N and F, where:

$S = (M \hat{} \ e) \bmod N$

$N = p * q$

M is an integer result of a one way checksum of the message text m

p, q and e are prime numbers chosen by the signatory, with p>q>e, and e coprime to (p−1)(q−1) ; and

F is an integer satisfying $((x \hat{} \ e) \hat{} \ F) \bmod N = x$ for all integers x.

The numbers p, q and e are the signatory's secret key. Only the signatory can easily calculate the signature S to match the text message m, and only the signatory can calculate the public key numbers N and F. However, anyone can verify that the signature S does indeed match the text m with the knowledge of the public key numbers N and F.

The security of the digital signature depends on the length of the number S. It is preferred that this number be at least 100 characters in length, and more preferably at least

about 300 characters in length. Even greater security may be desired for a value note issuer's signature, and a correspondingly longer signature may be provided for the value note issuer. The bearer and value note issuer signatures do not have to be the same length.

Fig. 2 shows an example representation of a value note 20. Essentially, the value note is a message which includes at least public key information 22 for the bearer, a currency value 24 which the value note represents, and a signature S_{BANK} 26 which endorses the bearer's public key information 22 and the value 24. In this embodiment, the value note 20 also includes a reference number or code 28 selected by the bearer, the name 30 of the issuing bank, a bank reference number or code 32 which uniquely identifies the value note to the bank, a "valid from" date 34 and an expiry date 36 which is the date by which the value note has to be redeemed.

The bank's new name information may include an e-mail address for the particular bank computer which issued the value note. As indicated in phantom in Fig. 2, the same bank may employ several autonomous computer systems to increase value note handling capacity. Each system will be able to handle value notes it has issued more efficiently than notes issued by a sister computer system. The e-mail address informs the bearer which computer is responsible for that value note.

Essentially, the value note is a promise by the issuing bank to pay the bearer the currency value 24 on redemption of the value note 20. As depicted in Fig. 2, the bank's signature S_{BANK} may optionally be based on one or more of the further items of information in the value note 20 in addition to the bearer's public key 22 and the note value 24. For example, the further information may include one or more of: the information 32 representing the bank's reference number; the "valid from" date 34; and the expiry date 36.

Referring to Fig. 3, the bank computer 10 issues a value note 20 in response to a request received from a user terminal 12. In order to make the request, the user has to transmit his public key information 22, the desired note value 24 and, if desired, a reference number 28. Referring to Fig. 3, the bank computer receives this request at step 40 and verifies that the user had paid the necessary funds to buy the value note. For example, the user may

request a debit from his account held by the bank. At step 42, the bank computer compiles the necessary information for the value note and, at step 44, the bank computer 10 calculates a bank signature based on the information in the value note, using the bank's secret key. At step 46, the bank computer 10 transmits the issued value note through the network 14 to the appropriate user terminal 12 to provide the user with the value note.

When making the request, the user may either send an empty or blank value note with his public key 22, the value 24 and the reference number 28 filled in, or the user may simply send the necessary information in a different form.

Once the user has received the issued value note from the bank computer 10, the user or bearer is then able to use the value note in a transaction with a third party over the public communications system 14. In the following, the current bearer of a value note is referred to as the buyer, and the third party who is to receive funds from the buyer is referred to as the seller.

The actions performed by the buyer to effect a transfer of funds are illustrated in Fig. 7. These actions may be partly carried out by software in the buyer's computer terminal, under the buyer's instructions.

Before the transaction between the buyer and seller can take place, the buyer first obtains sufficient information from the seller to produce a new value note in favour of the seller (step 74 in Fig. 7). As shown in Fig. 4, the information may be transmitted to the buyer in the form of a blank value note 50, and include information representing the seller's public key A_{SELLER} 52, the value 54 of the funds to be transferred to the seller, and a reference code 56 chosen by the seller.

Referring to Fig. 5, the buyer also prepares himself a new blank value note (step 75 in Fig. 7) which will represent the "change", ie. the remaining funds from the original value note 20, once the transaction has been effected. In a similar manner to the seller's blank value note, the buyer's new value note includes information representing a public key 62 for the buyer, the value 64 of the "change", and a new reference number 64 selected by the buyer.

In many cases, the public key information 62 provided in the buyer's new value note 60 will be the same as the public key information 22 provided in the original value note 20. However, this need not necessarily be the case. The buyer is free to choose a new secret key and an associated public key 62, and he may decide to do this to provide a greater degree of anonymity.

The next step (step 76 in Fig. 7) is for the buyer to append payment instruction information 68 to the value note 20, as illustrated in Fig. 6. In the present example, the payment instruction information instructs the bank to split the money value of the original value note 20 between the new value note 50 for the seller, and the new value note 60 for the buyer. The payment instruction information can identify each of the new value notes 50 and 60 by means of the bearer's reference 56 and 66, respectively. Also in this example, the respective currency values have been included in the seller's new value note 50, the buyer's new value note 60, as well as in the payment instruction information 68. This redundancy may be useful to ensure that no errors or mistakes occur in the new value note and the payment instruction information. However, the information might instead be included only once, either in the payment instruction information 68, the buyer's new value note 60, or the seller's new value note 50. For example, the bank computer 10 would be able to calculate the necessary "change" from the original value information 24 and the payment value 54 from the seller's new value note 50.

Finally, the buyer endorses the payment instruction information 68 (step 77 in Fig. 7) by calculating a digital signature 70 based on the payment instruction information 68 and on the buyer's secret key. As indicated in Fig. 6, one or more of the buyer's reference number 28, the buyer's public key 22, the "valid from" date 34, the expiry date 36 and the current date 72 may also be included in the information upon which the signature calculation is performed, to prevent such information from being tampered with fraudulently.

It is most preferable that the buyer's endorsement signature 70 be based on information including the currency values of the new value notes to be issued, to ensure that this information cannot subsequently be altered. If the currency values have been omitted from the payment instructions 68 and are specified instead on the blank value notes 50 and 60, then

the signature 70 should be dependent on the currency value information 54 and 64 specified in the blank value notes.

Having "signed" the value note 20, the buyer would then transmit the endorsed value note 20, the blank new buyer's value note 60 and the blank new seller's value note 50 through the communication network 14 to the bank computer 10 (step 78 in Fig. 7).

Referring to Fig. 8, the bank computer performs a number of verification tests upon the endorsed value note 20 (Fig. 6) to determine its authenticity. The order in which the tests are performed is not important; if any one of the tests fails, then the bank computer 10 may treat the value note as being "false", and need not honour the value note.

In this example, the bank computer 10 first performs a test 80 upon the "valid from" date information 34 and the expiry date information 36 in the received original value note 20, to ascertain whether the current date falls within an allowable window.

Assuming that the date is satisfactory, the bank computer 10 next proceeds to step 82 at which the buyer's signature 70 is analyzed. By using the public key information 22 originally presented in the value note 20, the bank computer 10 attempts to verify that the signature information 70 matches the information in the value note 20 upon which the signature information 70 is based. As explained above, the signature information 70 depends at least upon the payment instruction information 68, and may also depend on other predetermined information in the value note.

The test 82 will only be satisfied if: (i) the signature information 70 has been correctly calculated using the same secret key as that used to derive the public key information 22; and (ii) the information protected by the signature 70 (i.e. at least the payment instruction information 68) has not been altered. If the payment instruction information 68 (or the other information protected by the signature 70) has been altered, or if the signature 70 has itself been forged, then the information will fail the buyer's signature test 82.

Assuming that the buyer's signature test 82 is satisfied, the program then proceeds to

step 84 at which the bank computer 10 attempts to verify the original bank signature 26 against the information protected by that signature (in particular the buyer's public key information 22 and the original note value 24). The test 84 can be performed by using the bank's public key (in the same way as the test 82 described above). Alternatively, the bank computer 10 may simply repeat the original signature calculation to test whether an identical signature 26 is produced. If the test 84 fails, then this is an indication that at least some of the original information in the value note 20 has been altered (possibly either the original value information 24 or the original buyer's public key 22), and that the value note 20 should not be honoured.

If the above tests 80, 82 and 84 are all satisfied, this is indicative that the original value note 20 has not been tampered with, and that the buyer is the correct bearer authorised to redeem the value note. The next test 86 performed by the bank computer 10 ascertains whether the value note 20 has previously been redeemed. This test can be performed by comparing the bank's reference code 30 in the value note 20 with a list maintained in the bank computer 10 of each value note and the date, if any, of redemption. The purpose of this test 86 is to prevent a user from "double spending" a value note.

Assuming that the value note 20 has not previously been redeemed, the bank computer records the current date as the date of redemption, and proceeds to step 88 at which the new seller's value note 50 is completed and a bank's signature added to authenticate the new value note 50 in the same manner as that described above for the value note 20. The completed seller's value note is illustrated in Fig. 9. This is similar to the original form of value note 20 shown in Fig. 2, and the same reference numerals (followed by the letter "s") are used to indicate the corresponding information in the completed value note 50.

Similarly, at step 90 (in Fig. 8), the new buyer's value note 60 is completed and a bank's signature is added to authenticate the new buyer's value note 60. The completed new buyer's value note 60 is illustrated in Fig. 10, and corresponding reference numerals (followed by the letter "b") denote the value note information described previously.

At step 92 (in Fig. 8), the bank computer 10 completes the original value note 20 to

provide a receipt of the transaction to the buyer. The completed original value note 20 is illustrated in Fig. 11. This includes an "OK" message indicated at 94, and a final bank signature 96. The final bank signature is calculated based on the text of the buyers's signature 70 described above, and acts as a guarantee that the buyer's signature cannot subsequently be altered, either by the bank or by the buyer, should a dispute arise later. As indicated in Fig. 11, the final bank signature 96 may also be based on other information in the value note 20, such as the "valid from" information 32, the payment instruction information 68, and the "OK" message 94, to prevent alteration of those items of information in case of a dispute later.

Finally, at step 98 (in Fig. 8), the bank computer 10 transmits the new seller's value note 50, the new buyer's new value note 60 and the completed original value note 20 to the buyer's computer terminal. This is the computer terminal from which the original transaction instructions were transmitted to the bank computer 10. Upon receipt of the new value notes, the buyer would keep his own new value note 60 for further use, and forward the new seller's value note 50 to the seller as payment. The buyer's computer terminal would typically communicate with the seller's computer terminal through the public communication system 14 to transfer the seller's value note 50.

It will be appreciated that the above technique offers complete security even if the buyer and the seller do not know or trust each other, and even if the electronic messages are intercepted by another party.

In particular, if a thief intercepts the value note and attempts to redeem the value note with a forged signature, then the value note will fail the bank computer's test 82, since only the true bearer of a value note is able to calculate a correct signature with the knowledge of his secret key.

If a thief attempts to substitute his own public key in place of the original public key information 22 (in order to forge a "verifiable" bearer signature 70), then the value note will fail the bank computer's test 84 since the public key information 22 will no longer match that endorsed by the original bank signature 26.

Should an unscrupulous buyer attempt to forge a value note to send as payment to a seller, the seller would be able to identify this as a false value note from a simple "verification" of the forged bank signature 26 which will not match the public key information for the bank.

Any value note can be copied or distributed without increasing the liability of the bank, since the bank only has to honour the first valid presentation of a value note endorsed with payment instructions and a correct signature. The bank cannot avoid honouring at least one presentation, since it will not be able to demonstrate any other payment instructions except those correctly endorsed with the bearer's signature. If the bank is queried over the disposal of any issued note, the bank will be able to issue confirmation copies of the receipt value note 20 (Fig. 11), the seller's value note 50 (Fig. 9) and the buyer's replacement value note 60 (Fig. 10) without increasing its liability.

It will further be appreciated that the buyer and the seller can remain completely anonymous to the bank. The buyer's secret key(s) and the seller's secret key can be chosen quite arbitrarily so that they do not identify the buyer or the seller. In the example described above, the seller does not need to communicate directly with the bank computer 10, which further isolates the seller from the bank.

The only transactions which are not anonymous are:

(i) an initial transaction in which a payer is "buying" a new value note from an issuing bank using a payment from his bank account (discussed above with reference to Fig. 3); and

(ii) a final transaction in which a payee redeems a value note by including payment instruction information 68 to pay the value note into a bank account.

In either of the above, the identity of the bearer will be known to the bank because the bearer has to supply details of his bank account to the bank to effect the payment.

Apart from the above, a bearer of a value note does not need to be registered with or even have an account with the issuing bank. A user can receive and transfer value notes with

the anonymity and flexibility of cash in his hand.

A bearer does not even need to provide any personal information to the bank at all. The only information which a bearer is obliged to supply is his public key information, which can be selected or generated arbitrarily.

A further advantage is that the value notes permit division of the funds independently of the denomination of the funds. For example, a value note may even be calculated to fractions of a cent. A bearer may also combine two or more individual value notes into a new accumulated value note by a similar process to that described above. Essentially the bearer would endorse each individual value with the appropriate redemption instructions and send the collection of the individual value notes to the bank computer with a new blank value note to be returned with the accumulated value. It will be appreciated that electronic money or other commodity can be stored much more efficiently by value notes than by other conventional techniques, such as by e-cash where a number of indivisible electronic coins each need to be stored separately. The ability to divide, or to combine, value notes therefore provides extremely important advantages.

Should the user's computer 12 lose contact with the bank computer 10 during a transaction (such that the user does not know whether the transaction has been completed), the user can simply re-transmit the data to the bank computer 10 without increasing either his own liability, or the bank's liability.

In the above, the "valid from" information in the new value notes 50 and 60 may simply represent the instantaneous date and/or time of issuance, as a record of the date and/or time of issuance. Alternatively, the "valid from" information of one or both of the new value notes 50 and 60 may be set a predetermined interval after the time and/or date of issuance. This is equivalent to "post-dating" the value note so that it cannot be used again for immediate redemption. A possible advantage of this is that it can prevent a malicious user from repeatedly submitting new value notes for redemption immediately after issuance, and thereby try to overload the bank's computers. The interval may, for example, be from a few minutes, or less, to a day, or longer, as desired.

As a modification of the above embodiment, the buyer may send payment instructions to the bank computer 10 to issue a temporary value note with a limited life. This is illustrated in Figs. 12 to 17.

In a similar manner to that described previously, a buyer first obtains an empty or blank value note 50 from the seller (Fig. 4). However, the buyer now prepares himself two new value notes, each of the form shown in Fig. 5. The first of these will provide the change from the transaction in the same manner as that described previously, and the other will provide a replacement value note for the buyer if the seller fails to redeem the temporary value note within the set period.

Referring to Fig. 12, the buyer appends payment instruction information 100 to the original value note 20, in a similar manner to that described previously. However, the payment instruction information 98 instructs the bank computer 10 to create a only temporary value note (ie. an option note) having a limited life. The payment instruction information further includes a delayed instruction that, if the option note is not redeemed by the seller by an expiry date selected by the buyer, then the bank computer is to return the funds by issuing a second value note to the buyer.

The buyer then endorses the payment instructions with a digital signature 70, as described previously.

Before the buyer sends the endorsed value note 20 and the new blank value notes to the bank, the buyer appends further information to the seller's blank value note 50 to transform it into a blank "option" note 100. Referring to Fig. 13, the buyer adds option note information 102 about any further conditions or requirements which the seller must meet before the option note can be redeemed by the seller. Examples of such conditions are described below. The buyer may also include the expiry date information 104 for the option note (although these could also be included by the bank computer 10 later if desired). Finally, the buyer calculates a signature 106 based at least on the option note information 102 to endorse the option note information and prevent this from being altered later. As indicated in Fig. 13, the signature 106 may also be based on other information in the option note, such

as the seller's public key 52, the value 54 of the option note, and the expiry date 104, to protect these other items of information.

The buyer then transmits the modified seller's value note (ie. the blank option note in Fig. 13) with the endorsed value note 20 and the buyer's two blank value notes, to the bank computer 10.

Fig. 14 illustrates the completed value note 20 which the bank computer 10 returns to the buyer. This is similar to that shown in Fig. 11, and includes an "OK" message 94, and a final bank signature 96 to "sign off" the value note 20.

Fig. 15 illustrates the first new value note 69 for the buyer, which the bank computer returns to the buyer as the "change" from the transaction. This is exactly similar to that in Fig. 10.

Fig. 16 illustrates the option note 110 returned from the bank computer 10 for the seller. This is based on the option note 100 shown in Fig. 13, and further includes the bank's issuing information included in the other value notes, and denoted by corresponding reference numerals (followed by the letter "o").

If the seller decides to redeem the option note 110, ie. to take up the "option" presented in that note, the seller first has to meet the requirements or conditions in the option note information 102.

As one example, the option note information may be a requirement to obtain a further buyer's signature before the seller can redeem the option note. This can provide a useful "counter-signing" feature to enable the buyer to finally confirm that the option note may be redeemed.

As another example, the option note information may represent a receipt, or other information, which the seller has to endorse with a signature as part of the redemption process. This provides a useful technique for obtaining a certified recept for the transaction

from the seller.

Fig. 17 illustrates an endorsed option note 110 which includes both of the above examples of option note information. The value note includes a signature 112 calculated by the seller to endorse the option note information 102, or at least a receipt string part of the option note information. In this embodiment, the receipt string comprises encrypted text so that neither the bank computer 10 nor bank staff can read the receipt text. This provides absolute anonymity for the transaction at the same time as providing a receipt decipherable by the buyer and seller.

As an example, the receipt text may be encrypted by being "blinded" by the use of a blinding function. This is a function which renders the text unreadable, but which preserves a relationship with a signature, such that the signature can be verified against the blinded text in exactly the same way as described above against unblinded text. An example of a blinding function, which is related to the RSA signature function described hereinbefore is as follows:

By using the known public key information N and F for the seller, the buyer "blinds" the text t by applying a blinding function T = (t ^ F) mod N. The seller then selects an arbitrary integer y, and calculates Y = (y ^ F) ^ F mod N. Finally the buyer calculates M' = M * (y ^ F) mod N. The message T is the blinded text, and the values M' and Y accompany this.

When this information is sent to the seller, the seller can calculate y = (Y ^ e) ^ e mod N, and t = (T ^ e) mod N to read the blinded message, and can verify that the original checksum M = M'/(y ^ F) mod N matches the original message t. Then the seller can calculate a signature S on the blinded text T in the same manner as before, as S = (M' ^ e) mod N.

When the blinded message T, the signature S and the accompany information M' and F are sent to the bank computer, the bank computer can verify that the signature is valid by verifying that S = (M' ^ F) mod N. In this manner, the bank can verify that the seller has signed the message to the buyer, even though the bank is not able directly to read the blinded

message T.

The buyer can calculate:

S/Y mod N

= (M' ^ e) / y mod N

= ((M * (y ^ F)) ^ e) / y

= (M ^ e) * Y / Y

= s (which is the signature for the message t). Even if the bank later sees t and s, along with many other similar texts and signatures of the seller, it will be impossible for the bank to correlate these to the blinded text T and blinded signature S.

The option note also includes a second signature 114 calculated by the buyer, to meet the requirement in the option note information 102. The buyer's second signature should be calculated using text information in the option note different from that protected already by the buyer's endorsing signature 106. In this embodiment, the buyer's second signature is based on text comprising the bank's issuing signature 26.

The option note finally includes payment instruction information 68 from the seller to the bank, and a seller's signature 116 endorsing the payment instruction information 68. The seller must complete the option note as described above, and transmit the option note to the bank 10 before the option note expires. Assuming that the seller meets these requirements, then the bank computer 10 is obliged to redeem the option note in accordance with the seller's payment instructions. However, if the seller fails to redeem the option note by the expiry date, then the bank computer 10 will complete the buyer's second blank value note to return the funds to the buyer.

Fig. 18 illustrates the additional test steps carried out by the bank computer 10 when an option note is returned by a seller for redemption. These are additional to the date and authenticity tests shown in Fig. 8.

In step 120, the bank computer 10 first tests whether the option note conditions include a requirement for the buyer to countersign the option note. If not, the routine branches

to step 124. If the buyer's countersignature is required, the routine proceeds to step 122 which tests whether the buyer's counter signature 114 has been included, and is valid.

After step 122, the bank computer proceeds to step 124 at which bank computer 10 tests whether the option note conditions include a requirement for the seller endorse a text message (for example, an encrypted receipt message) with the seller's signature. If not, the routine branches past step 126 to indicate that the option note conditions have been met. If a seller's signature is required, step 126 tests whether it matches the receipt text provided by the buyer.

If either of the signature tests at steps 122 and 126 fails, then the routine indicates that the option note is false, or at least has failed the option note conditions, and is not to be redeemed.

After the expiry date of the option note, the buyer may contact the bank computer 10 to enquire about the option note. For example, the buyer may submit a copy of the option note as evidence of authorization. If the seller has not redeemed the option note, the bank computer 10 can issue the new value note to the buyer at that stage to return the funds. On the other hand, if the seller has redeemed the option note, then the bank computer can provide a copy of the fully signed option note (Fig. 17) to the original buyer as a receipt for the transaction (which includes the receipt information presented in the option note information 102).

In this and the previous embodiment described above, should any of the tests 80 to 86, 122 and 126 fail, then the bank computer 10 should not honour the value note for redemption. In this case, the bank computer 10 may issue a reply in a similar manner to the completed value notes illustrated in Figs. 11 and 14, with the "OK" message replaced by a "NOT OK" message together with a further text message explaining why the transaction has failed. By endorsing this message with a digital signature, the bank computer 10 can ensure that the "failed" message cannot be tampered with after issuance by the bank computer 10.

In addition to the advantages previously described, the option note techniques provide

a powerful transaction tool. In particular, the seller cannot deny that he has received the funds from the buyer. In redeeming the option note, the seller can be forced to provide a receipt for the funds which the seller has to sign as part of the option note requirements. By encrypting the receipt message, the details of the transaction receipt can be kept confidential from the bank. However, the bank computer is able to verify whether the seller's signature endorsing the receipt text is valid.

If desired, the buyer can specify which signature the seller has to use, to "test" whether the seller's identity is genuine. For example, if the seller is a company which publishes its public key information, the buyer can insist that the seller uses its signature based on the published public key information. Only a genuine company with knowledge of the secret key to match the public key will be able to correctly calculate a matching signature.

A further advantage is that if the buyer prepares one or more option notes in advance of potential transactions, the transactions can be performed "offline" from the bank computer. The buyer may, for example, print the or each option note on paper, and send or hand the option note to the seller. The seller will then have a certain period (for example, a few days) to make contact with the bank computer to redeem the option note (which is guaranteed up to that time). However, if for any reason the buyer decides not to proceed with any of the transactions and keeps the option notes for those transactions, the bank will simply return the funds to the buyer by issuing new value notes when the option notes expire. In this case, the seller never obtains the option notes.

A further advantage is that a buyer and a seller can swap notes in a secure manner. The ability to swap notes may be desirable to further improve the anonymity of the bearer's of the value notes. A swapping authority could be established on, for example, the internet to allow bearers to submit value notes for swapping, and to receive replacement anonymous notes in return.

For example, a buyer may write a first option note which requires a further buyer signature before the option note can be redeemed. A seller may write a second option note whose receipt text is the buyer's note, and which requires the buyer's signature to this receipt.

The buyer and the seller may then swap the option notes so that the buyer and the seller each possess each other's option note. When the buyer spends the seller's option note, the buyer has to provide the buyer signature on the option note. Through the bank, this signature would be made available to the seller (as receipt information) to enable the seller now to spend the buyer's option note.

It will be appreciated that the above description is merely illustrative of preferred examples of the invention. The information making up the value notes may be presented in any desired form, and need not be in the same order as that described above.

Although in the above embodiments the value notes have represented money, value notes may be used to represent any form of commodity, whether transferable or not. For example, value notes could be used to represent transferable bearer bonds, nominee shares, options and derivatives, to enable transfers or trading over the internet. In another example, value notes could be used to represent a lottery ticket, the commodity then being the selected lottery numbers. This would provide a secure method of selling lottery tickets over the internet, while guaranteeing that the lottery number information cannot be tampered with once the lottery value note "ticket" has been issued. These are merely examples of a wide variety of applications for value notes in accordance with the present invention.

CLAIMS

1. A method of providing a value note comprising:
providing first information representative of public key information for a bearer;
providing second information representative of a commodity represented by the value note; and
calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of public key information for the issuer.

2. A method according to claim 1, further comprising providing information on when the value note is due to expire.

3. A method according to claim 2, wherein the expiry information is included in the calculation of the signature.

4. A method according to claim 1, 2 or 3, further comprising providing identification information for uniquely identifying the value note.

5. A method according to claim 4, wherein the identification information comprises a serial identification string.

6. A method according to claim 4 or 5, wherein the identification information is included in the calculation of the signature.

7. A method according to any preceding claim, further comprising sending the value note electronically.

8. A method according to claim 7, wherein the value note is sent through an electronic public communication system.

9. A method of handling a value note, comprising:
receiving a value note comprising first information representative of a bearer's public

key, second information representative of a commodity represented by the value note, and third information representing an issuer's signature which can be verified by information including the first and second information and public key information for the issuer;

providing redemption instruction information for the value note; and

providing a bearer's signature which is dependent on the payment instruction information and is verifiable from said first information.

10. A method according to claim 9, wherein the step of providing the bearer's signature comprises calculating the signature based on information including the redemption instruction information and a secret key related to the first information.

11. A method according to claim 10, wherein said information on which the bearer's signature is calculated includes information from the value note.

12. A method according to claim 9, 10 or 11, wherein the redemption instruction information includes a reference to transfer at least a proportion of the commodity to a first new value note.

13. A method according to claim 12, wherein the first new value note has a different bearer's public key from the value note being redeemed.

14. A method according to claim 12 or 13, wherein the redemption instruction information includes a reference to transfer the remainder of the commodity to a second new value note.

15. A method according to claim 14, wherein the second new value note has a different bearer's public key from the value note being redeemed.

16. A method according to claim 12, 13, 14 or 15, wherein the redemption instruction information includes a reference to transfer the commodity represented by the first new value note to a third new value note if the fist new value note is not redeemed within a predetermined period.

17. A method according to claim 16, wherein the third new value note has a different bearer's public key from the first new value note.

18. A method according to any of claims 10 to 17, further comprising communicating the value note, the redemption instruction information and the bearer's signature information to a value note handling authority.

19. A method according to claim 18, wherein the communication is effected over an electronic public communication system.

20. A method of handling a value note with associated redemption instruction information and bearer signature information, the method comprising performing at least one verification prior to redeeming the value note in accordance with the redemption instruction information, the verification comprising:

verifying that the bearer signature information matches information including at least the payment redemption instruction information using public key information for the bearer presented in the value note.

21. A method according to claim 20, further comprising verifying that an issuer signature included in the value note matches information including the bearer public key information and the commodity represented by the value note, using public key information for the issuer.

22. A method according to claim 20 or 21, further comprising verifying that the value note has not previously been presented for redemption.

23. A method according to claim 22, wherein the value note includes identification information for uniquely identifying the value note, and the verification comprises ascertaining whether a value note bearing the same identification information has previously been presented for redemption.

24. A method according to claim 20, 21, 22 or 23, further comprising verifying whether a counter signature matches public key information in the value note for a counter signatory.

25. A method according to claim 20, 21, 22, 23 or 24, further comprising verifying whether an endorsement signature in the value note matches information including a predefined message using public key information for the message endorsing signatory.

26. A method according to any of claims 20 to 25, wherein the value note includes expiry time and/or date information representing a time and/or date of expiry, and the method further comprises testing the value note on the basis of the expiry information.

27. A method according to any of claims 20 to 26, wherein the value note includes valid–from time and/or date information representing a time and/or date from which the value note may validly be redeemed, and the method further comprises testing the value note on the basis of the valid–from information.

28. A method according to any of claims 20 to 27, wherein the step of redeeming the value note comprises issuing a first new value note representing at least a proportion of the commodity of the value note being redeemed.

29. A method according to claim 28, wherein first new value note includes different public key information from the value note being redeemed.

30. A method according to claim 28 or 29, wherein the step of redeeming the value note comprises issuing a second new value note representing the remainder of the commodity of the value note being redeemed.

31. A method according to claim 30, wherein the second new value note includes a different bearer public key from the value note being redeemed.

32. A method according to claim 28, 29, 30 or 31, wherein the step of redeeming the value note comprises issuing a third new value note if said first new value note is not redeemed within a predetermined period.

33. A method according to claim 32, wherein the third value note includes a different

bearer's public key from the value note being redeemed.

34. A method according to any of claims 28 to 33, wherein at least one new value is issued which includes information indicative of a time and/or date from which the new value note can be redeemed, and wherein the time and/or date is later than the time and/or date, respectively, of issuance.

35. A method according to any of claims 20 to 34, further comprising communicating the or each new value note electronically to a remote party corresponding to the source of the value note being redeemed.

36. A method according to claim 33, wherein the communication is effected over a public communication system.

37. A method wherein an electronic representation of a commodity is issued by an issuing authority, the electronic representation including information representing a time and/or date from which the electronic representation is available for redemption, said time and/or date being later than the time and/or date of issuance, whereby the electronic representation is not available for redemption immediately after issuance.

38. A method of encrypting data, comprising:

applying a blinding function to the data to encrypt said data using first secret key information;

calculating a digital signature using a signature function which is dependent firstly on said blinded data or on blinded hashing information calculated from unblinded data, and secondly on second secret key information, in such a manner that the signature is verifiable using public key information related to the second secret key;

composing a message including the encrypted data, the digital signature, and encrypted information relating to the first secret key;

whereby it is possible to verify from said encrypted data and from said digital signature that the signature matches the encrypted data without decrypting the encrypted data, and whereby, with knowledge of the encryption used to encrypt the first secret key

information in the message, it is possible to ascertain the first secret key information and to decrypt said encrypted data.

39. A method of encrypting and transmitting data, comprising:

applying a blinding function to the data to encrypt said data using first secret key information;

composing a first message including the encrypted data and encrypted information relating to the first secret key;

transmitting the first message to a first receiver;

calculating a digital signature using a signature function which is dependent firstly on said blinded data or on blinded hashing information for the unblinded data, and secondly on second secret key information, in such a manner that the signature is verifiable using public key information related to the second secret key;

composing a second message including the encrypted data, the encrypted information relating to the first secret key and the digital signature;

transmitting the second message to a second receiver.

40. A method according to claim 39, further comprising calculating said hashing information for the unblinded data and including said hashing information in the first message.

41. A method according to claim 39 or 40, further comprising the following steps after receipt of the first message by the first receiver:

de-crypting the encrypted information relating to the first secret key; and

un-blinding the encrypted data using the de-crypted first secret key information.

42. A method according to claim 39, 40 or 41, further comprising the following step after receipt of the second message by the second receiver:

verifying whether the digital signature matches the encrypted data.

43. Apparatus for carrying out a method as defined in preceding claim.

44. A value note comprising:

first information representative of public key information for a bearer;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and public key information for the issuer.

45. A record carrier which is recorded value note information including:

first information representative of public key information for a bearer;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and public key information for the issuer.

46. A transmission signal representing a value note and comprising:

first information representative of public key information for a bearer;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and public key information for the issuer.

ABSTRACT

IMPROVEMENTS RELATING TO ELECTRONIC TRANSACTIONS

Methods and apparatus are disclosed for effecting transfers using an electronic representation of a commodity, such as money. The commodity is represented by a value note issued by a bank or other authority, and which includes:

first information representative of public key information for a bearer;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and public key information for the issuer.

Digital endorsement signatures are used to redeem one value note for one or more others, and to authenticate information in the value notes to prevent alteration.

(Fig. 6)

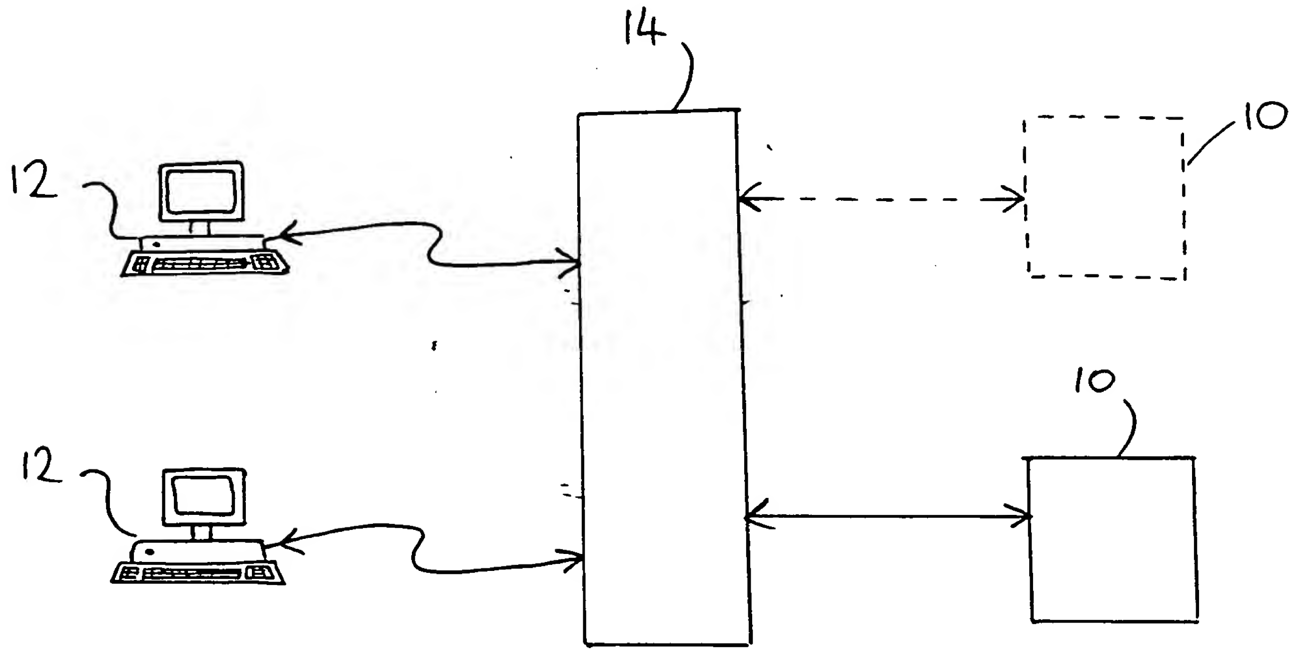


Fig. 1

This Page Blank (uspto)

20

28 buyer's reference number
22 buyer's signature = A_{BUYER}
24 value of note
30 bank's name
32 bank's reference number
34 valid from date
36 valid to date
26 bank's signature = S_{BANK} {22, 24 [32, 34, 36]}

FIGURE 2

60

66 buyer's reference number
62 buyer's signature = A_{BUYER}
64 value of note

FIGURE 5

50

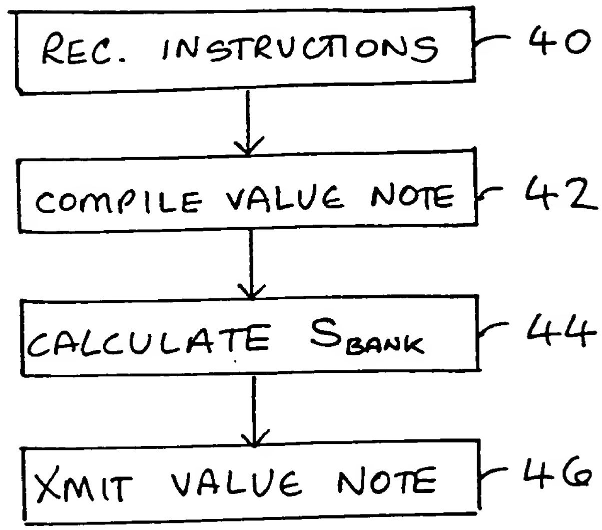
56 seller's reference number
52 seller's signature = A_{SELLER}
54 value of note

FIGURE 4

20

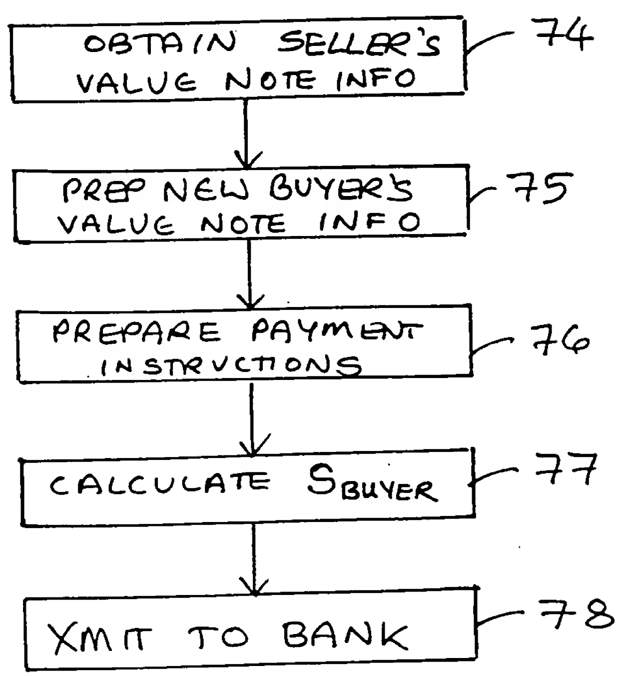
buyer's reference number
buyer's signature
value of note
bank's name
bank's reference number
valid from date
valid to date
bank's signature
68 instructions e.g.
"please pay the sum v on <note x>
and give change on <note y>"
72 today's date
70 buyer's second signature S_{BUYER} {68 [28, 22, 34, 36, 72]}

FIGURE 6



REC. INSTRUCTIONS
40
COMPILE VALUE NOTE
42
CALCULATE S_{BANK}
44
XMIT VALUE NOTE
46

FIG. 3



OBTAIN SELLER'S VALUE NOTE INFO
74
PREP NEW BUYER'S VALUE NOTE INFO
75
PREPARE PAYMENT INSTRUCTIONS
76
CALCULATE S_{BUYER}
77
XMIT TO BANK
78

FIG. 7

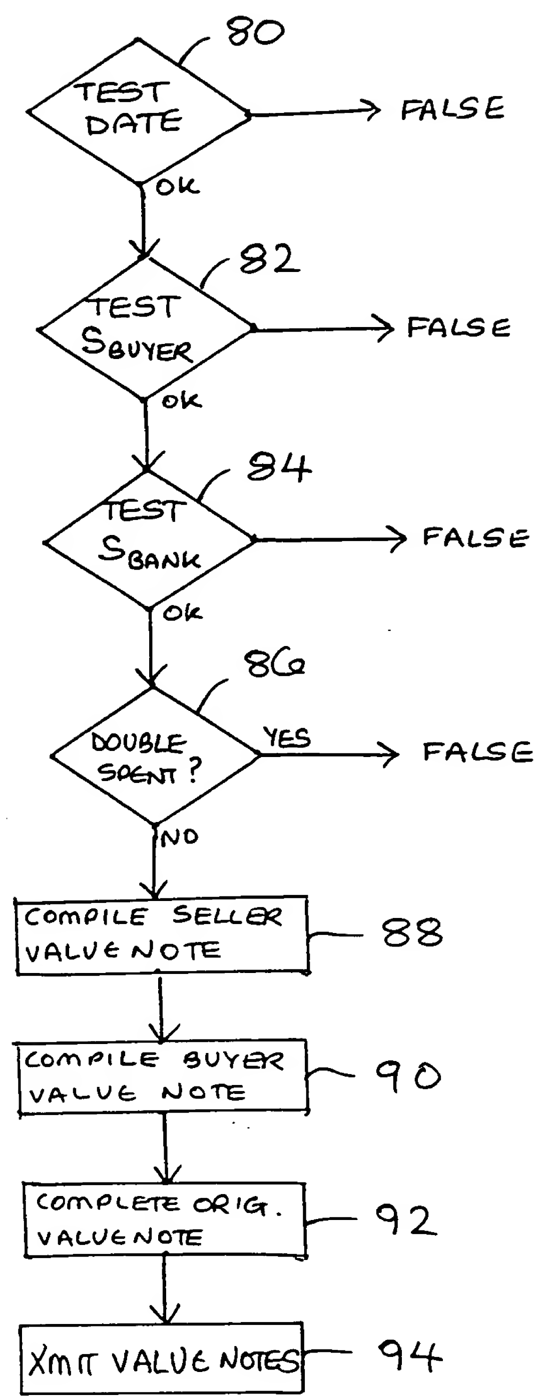

80
TEST DATE
FALSE
OK
82
TEST S_{BUYER}
FALSE
OK
84
TEST S_{BANK}
FALSE
OK
86
DOUBLE SPENT ?
YES
FALSE
NO
COMPILE SELLER VALUE NOTE
88
COMPILE BUYER VALUE NOTE
90
COMPLETE ORIG. VALUE NOTE
92
XMIT VALUE NOTES
94

FIG. 8

50

28s seller's reference number
22s seller's signature A_{SELLER}
24s value of note
30s bank's name
32s bank's reference number
34s valid from date
36s valid to date
26s bank's signature = S_{BANK}

FIGURE 9

60

28b buyer's reference number
22b buyer's signature = A_{BUYER}
24b value of note (change)
30b bank's name
32b bank's reference number
34b new valid from date
36b new valid to date
26b bank's signature S_{BANK}

FIGURE 10

20

buyer's reference number
buyer's signature
value of note
bank's name
bank's reference number
valid from date
valid to date
bank's signature
instructions =
"please pay <seller> the sum v on supplied note ref Z
and give change to <buyer> on supplied note y"
today's date
70 buyer's signature
94 OK
96 bank's signature = S_{BANK} {70 [32, 68, 94]}

FIGURE 11

buyer's reference number 20
buyer's signature
value of note
bank's name
bank's reference number
valid from date
valid to date
bank's signature
instructions: e.g.
100 "please give change on <note y> and
pay the sum v on <option note z>
to be exercised with receipt by <ex-date>
failing which refund the sum V on <note W>"
today's date
70 buyer's second signature

FIGURE 12

seller's reference number
52 seller's signature A_{SELLER} 50 (100)
54 value of note
102 buyers note requirements:
Receipt Information (possibly empty)
106 buyer's signature S_{BUYER} {102 [52, 54, 104]}
104 valid to date <ex-date>

FIGURE 13

seller's reference number 110
seller's signature
value of note v
102 buyers requirement including receipt string:
Receipt of <value> by <name of buyer>
buyer's signature
bank's name
bank's reference number
new valid from date
new valid to date <ex-date>
26 bank's signature S_{BANK}
Instructions: e.g.
68 "please pay the sum v on <note q>
today's date
112 seller second signature S_{SELLER} {102}
116 sellers receipt signature S_{SELLER} {68}
114 buyers approval signature S_{BUYER} {26}

FIGURE 17

20

buyer's reference number
buyer's signature A_{BUYER}
value of note
bank's name
bank's reference number
valid from date
valid to date
bank's signature = S_{BANK}
instructions: e.g.
"please give change on <note y> and pay the sum
v on <note z>
to be exercised with receipt by <ex–date>
failing which refund the sum v on <note w>"
today's date
buyer's second signature = S_{BUYER}
94 OK
96 bank's signature = S_{BANK}

FIGURE 14

69

buyer's reference number
buyer's signature = A_{BUYER}
value of note (change)
bank's name
bank's reference number
new valid from date
new valid to date
bank's signature = S_{BANK}

FIGURE 15

110

280 seller's reference number
220 seller's signature = A_{SELLER}
240 value of note = v
102 buyers note requirement with receipt string:
Receipt of <value> by <name of buyer>
106 buyer's signature = S_{BUYER}
300 bank's name
320 bank's reference number
340 new valid from date
360 new valid to date = <ex–date>
260 bank's signature = S_{BANK}

FIGURE 16

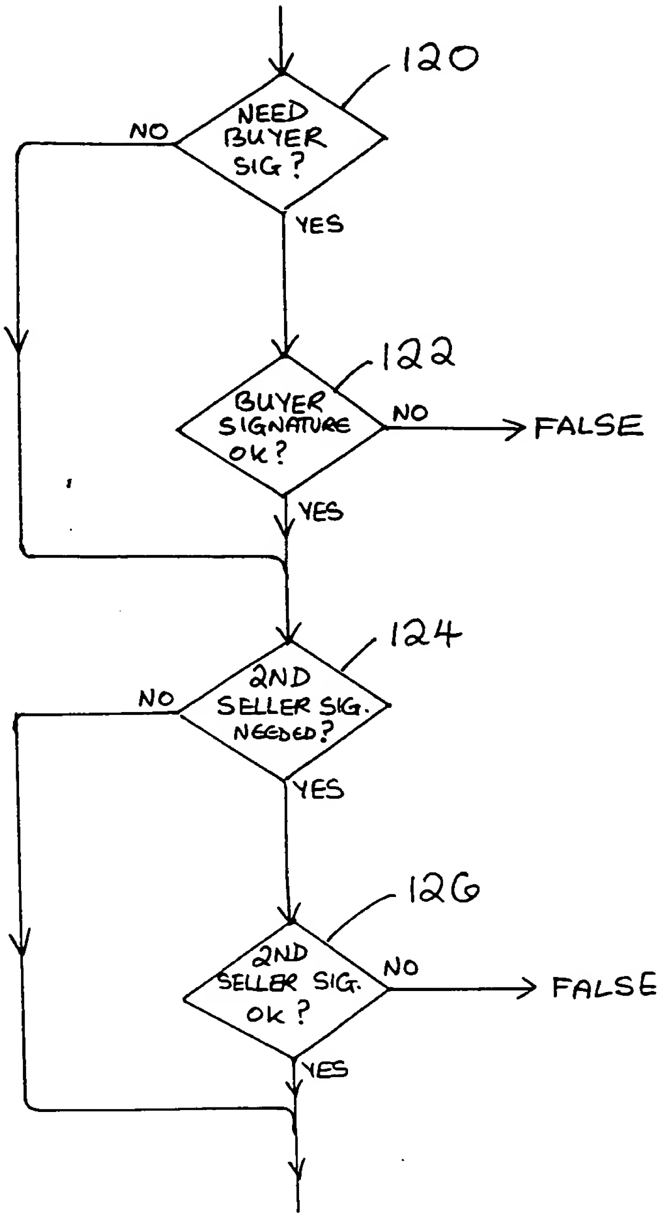

120
NEED BUYER SIG?
NO
YES
122
BUYER SIGNATURE OK?
NO
FALSE
YES
124
2ND SELLER SIG. NEEDED?
NO
YES
126
2ND SELLER SIG. OK?
NO
FALSE
YES

FIG. 18

PCT/GB97/02[illegible]2

D. YOUNG & CO.

(NO DATE STAMP)